IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises I.

1. *(3 points)*
   (a) Find the minimal distance of the code $C = \{11111, 00100, 10010, 01001\}$.
   (b) Using the code C, decode the strings $11011, 01101, 10011, 00111$ according to the nearest neighbor decoding strategy.

2. *(5 points)*
   (a) For any $N \geq 1$, find a binary code C_N with $(n, M, d) = (2N, 4, N)$.
   (b) For any $M_0 \geq 2$ and any $d_0 \geq 1$, find a binary (n, M, d) code with $M \geq M_0$ and $d \geq d_0$.

3. *(2 points)* Decide whether the following ternary (respectively binary) codes are equivalent.

   (a) $C_1 = \begin{Bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{Bmatrix}$ $C_2 = \begin{Bmatrix} 0 & 2 & 0 \\ 2 & 1 & 2 \\ 1 & 0 & 1 \end{Bmatrix}$ (b) $C_1 = \begin{Bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{Bmatrix}$ $C_2 = \begin{Bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{Bmatrix}$

4. *(6 points)* Show that if $d \geq \frac{n}{2}$ then $A_2(n, d) \leq 2n$.

   You can use the following lemma:

   Lemma. *Let $u_1, \ldots, u_m \in \mathbb{R}^n$ such that $|u_i| = 1$ and $u_i \cdot u_j \leq 0$ for all $1 \leq i < j \leq m$. Then $m \leq 2n$.*

5. *(5 points)* Consider the following code with codewords of length 6 over alphabet $\{0, \ldots, 9\}$ where the verification process is as follows:

   i. Multiply digits on even positions by 2 (starting from the rightmost digit).
   ii. Sum all the individual digits (both unchanged and doubled digits).
   iii. The codeword is valid if the sum modulo 10 is equal to zero.

   (a) Calculate the last digit x of $19054x$.
   (b) Given the first five digits show how to compute the check digit.
   (c) Can this code detect any single error?
   (d) Can this code detect any transposition error involving adjacent digits?

   Explain your answers.

6. *(4 points)* Consider a source X producing symbols A, B, C and D with the following probabilities:

symbol	probability
A	0.45
B	0.10
C	0.15
D	0.30

   Design a binary Huffman code and calculate its average codeword length and its efficiency.